UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/505,951	02/15/2000	Simon Robert Walmsley	AUTH08US	5608

7590 08/23/2005

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/505,951	WALMSLEY ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A Request for Continued Examination was received on 06 June 2005. No claims have been amended, added, or canceled. Claims 1-20 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-9, 11, and 14-19 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-3, 7, 9, 12, 13, 10, 11, 14, 15, 19, 22, 20, and 21, respectively, of U.S. Patent No. 6816968 (hereinafter "the conflicting patent"). Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1 and 11 of the present application are broader than corresponding Claims 1 and 14 of the conflicting patent. Specifically, Claims 1 and 11 of the present application are identical to Claims 1 and 14 of the conflicting patent, except the claims of the present application do not recite the limitations regarding a "data message". Further, the "prove function" of present Claims 6, 11, and 22 is broader than the corresponding "read function" in Claims 12, 14, and 22 of the conflicting patent, because the read function also includes limitations directed to the "data message" that are not included in the prove function. All other claims not specifically referred to correspond substantially in the order set forth above.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-4, 6-15, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Spies et al, US Patent 5689565.

In reference to Claim 1, Sony discloses an authentication method (see Figures 7-9, Claim 1, and column 2, line 49-column 3, line 17) in which a random number is generated (column 8, lines 12-17) and encrypted with a symmetric encryption function using a first key in a first apparatus (column 9, lines 13-17). The encrypted random number is sent to a second apparatus (column 9, lines 18-21) and decrypted with a symmetric decryption function using the first key (column 9, lines 31-37), and then encrypted with the symmetric encryption function using a second key (column 9, lines 41-48) and sent to the first apparatus (column 9, line 57-column 10, line 2). The encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28). The two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). However, Sony does not disclose the calculation and comparison of a digital signature as a step of the authentication method.

Spies discloses a cryptographic system and method that includes generating a digital signature of a document (column 12, lines 6-13) and encrypting the document and digital signature under the same symmetric encryption key in a sending device (column 12, lines 14-27, noting especially the equation at line 25). Spies further

discloses decrypting the document and signature at a receiving device (column 13, lines 15-22) and verifying the signature (column 13, lines 20-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Sony by including the steps of generating a digital signature of the random number (the "document") and encrypting the signature with the random number in the first apparatus, and of decrypting and verifying the signature in the second apparatus, in order to authenticate the sending of the random number (see Spies, column 13, lines 26-32) and more generally to allow for greater security, privacy, authenticity, and integrity in the system (see Spies, column 2, lines 1-4).

In reference to Claim 2, Sony further discloses that the first and second keys are held in both the first and second apparatuses (see Figure 9).

In reference to Claim 3, Sony further discloses that the first apparatus contains a random function to generate random numbers (column 8, lines 12-15).

In reference to Claim 4, Sony further discloses that the second apparatus holds a decryption function (column 9, lines 31-37).

In reference to Claim 6, Sony further discloses that the second apparatus decrypts the random number with the first key (column 9, lines 31-37), encrypts the random number with the second key (column 9, lines 41-48), and sends the encrypted random number to the first apparatus (column 9, line 57-column 10, line 2). Additionally, Spies further discloses verifying the signature in the second apparatus (column 13, lines 20-36).

In reference to Claim 7, Sony further discloses that the second apparatus monitors the time elapsed between steps of its processing (column 10, lines 53-56).

In reference to Claim 8, Sony further discloses that the function generating the random numbers is held in the first apparatus (column 8, lines 12-15). Additionally, Sony discloses that if the second apparatus is not authenticated, the authentication process is terminated (column 10, lines 36-39).

In reference to Claim 9, Sony further discloses that the first apparatus monitors the time elapsed between steps of its processing (column 10, lines 6-7).

In reference to Claim 10, Sony further discloses that it is determined if the second apparatus is valid (column 10, lines 31-35) or not (column 10, lines 36-39).

Claims 11-15 and 17-20 are system claims corresponding substantially to the methods of Claims 1-4 and 6-10, and are thus rejected by a similar rationale.

7. Claims 5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony in view of Spies as applied to claims 1 and 11 above, and further in view of Schneier, *Applied Cryptography*.

Sony as modified by Spies discloses everything as applied to Claims 1 and 11 above. However, Sony does not disclose the use of digital signatures, and Spies does not explicitly disclose the use of digital signatures of 160 bits. Schneier discloses that hash functions can be used in the creation of digital signatures, and specifically discloses the use of 160 bit hashes (page 38, last paragraph). Therefore, it would have

been obvious to modify the method of Sony and Spies to include digital signatures 160 bits in length in order to increase the speed of the signature algorithm (see Schneier, page 38, last paragraph-page 39, first full paragraph).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Krsul et al, US Patent 5839119, discloses methods that include sealing digitally signed messages by encrypting the signed message and signature using either asymmetric or symmetric encryption.

b. Schneier et al, US Patent 5956404, discloses digital signature methods along with authentication protocols involving signatures, random number generation and verification, and encryption of signatures and messages together under a symmetric key.

c. Sumner, US Patent 6009173, discloses cryptographic methods that include encrypting a signed message under a symmetric key.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER